FEDERAL TRADE COMMISSION

Consumer Information

consumer.ftc.gov

How to Keep Your Personal Information Secure

Protecting your personal information can help reduce your risk of identity theft. There are four main ways to do it: know who you share information with; store and dispose of your personal information securely, especially your Social Security number; ask questions before deciding to share your personal information; and maintain appropriate security on your computers and other electronic devices.

Keeping Your Personal Information Secure Offline

Lock your financial documents and records in a safe place at home, and lock your wallet or purse in a safe place at work. Keep your information secure from roommates or workers who come into your home.

Limit what you carry. When you go out, take only the identification, credit, and debit cards you need. Leave your Social Security card at home. Make a copy of your Medicare card and black out all but the last four digits on the copy. Carry the copy with you — unless you are going to use your card at the doctor's office.

Before you share information at your workplace, a business, your child's school, or a doctor's office, ask why they need it, how they will safeguard it, and the consequences of not sharing.

Shred receipts, credit offers, credit applications, insurance forms, physician statements, checks, bank statements, expired charge cards, and similar documents when you don't need them any longer.

Destroy the labels on prescription bottles before you throw them out. Don't share your health plan information with anyone who offers free health services or products.

Take outgoing mail to post office collection boxes or the post office. Promptly remove mail that arrives in your mailbox. If you won't be home for several days, request a vacation hold (http://www.usps.com/holdmail) on your mail.

When you order new checks, don't have them mailed to your home, unless you have a secure mailbox with a lock.

Consider opting out (/articles/0262-stopping-unsolicited-mail-phone-calls-and-email) of prescreened offers of credit and insurance by mail. You can opt out for 5 years or permanently. To opt out, call 1-888-567-8688 (tel:18885678688) or go to optoutprescreen.com (https://www.optoutprescreen.com/?rf=t). The 3 nationwide credit reporting companies operate the phone number and website. Prescreened offers can provide many benefits. If you opt out, you may miss out on some offers of credit.

Keeping Your Personal Information Secure Online

Know who you share your information with. Store and dispose of your personal information securely.

Be Alert to Impersonators

Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.

Safely Dispose of Personal Information

Before you dispose of a computer (/articles/0010-disposing-old-computers), get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive.

Before you dispose of a mobile device (/articles/0200-disposing-your-mobile-device), check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

Encrypt Your Data

Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.

Keep Passwords Private

Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.

Don't Overshare on Social Networking Sites

If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Securing Your Social Security Number

Keep a close hold on your Social Security number and ask questions before deciding to share it. Ask if you can use a different kind of identification. If someone asks you to share your SSN or your child's, ask:

- why they need it
- how it will be used
- how they will protect it
- what happens if you don't share the number

The decision to share is yours. A business may not provide you with a service or benefit if you don't provide your number. Sometimes you will have to share your number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. A business may ask for your SSN so they can check your credit when you apply for a loan, rent an apartment, or sign up for utility service.

Keeping Your Devices Secure

Use Security Software

Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.

Avoid Phishing Emails

Don't open files, click on links, or download programs sent by strangers**.** Opening a file from someone you don't know could expose your system to a computer virus or spyware (/articles/0011-malware) that captures your passwords or other information you type.

Be Wise About Wi-Fi

Before you send personal information over your laptop or smartphone on a public wireless network (/articles/0014-tips-using-public-wi-fi-networks) in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.

Lock Up Your Laptop

Keep financial information on your laptop (/articles/0009-computer-security)only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.

Read Privacy Policies

Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

July 2012

Related Items

- Sharing Information: A Day in Your Life (https://www.consumer.ftc.gov/media/video-0022-sharing-information-day-your-life)
- Five Ways to Help Protect Your Identity (https://www.consumer.ftc.gov/media/video-0023-five-ways-help-protect-your-identity)
- Identity Theft (https://www.consumer.ftc.gov/features/feature-0014-identity-theft)
- Computer Security (https://www.consumer.ftc.gov/articles/0009-computer-security)
- Phishing (https://www.consumer.ftc.gov/articles/0003-phishing)
- Protecting Your Child's Privacy Online (https://www.consumer.ftc.gov/articles/0031-protecting-your-childs-privacy-online)
- Stopping Unsolicited Mail, Phone Calls, and Email (https://www.consumer.ftc.gov/articles/0262-stopping-unsolicited-mail-phone-calls-and-email)